~~SECRET~~

ROUTING AND RECORD SHEET

SUBJECT: (Optional)

Computer Security

FROM: [redacted]

25X1

Director of Security

25X1 [redacted]

EXTENSION

NO.

DATE 4 FEB 1987

TO: (Officer designation, room number, and building)	DATE RECEIVED	DATE FORWARDED	OFFICER'S INITIALS	COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.)
1. D/OIT 2D-00 Headquarters				Gary has a copy and another routed to Lev + Orr — Gary, Let's send our version to DDP already sent.
2.				
3. DD/OIT-M				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				UNCLASSIFIED When Separated from Attachment

4 FEB 1987

MEMORANDUM FOR: Deputy Director for Administration

25X1 FROM: [redacted]
Director of Security

SUBJECT: Computer Security

1. The Office of Security and the Office of Information Technology share common goals regarding the security of CIA information systems. Progress toward those goals is being jeopardized by continuing uncertainty and debate over basic responsibilities. This memorandum offers a plan to clear the air and get us moving forward together.

2. The Action Plan: We believe that the following actions should be taken to get CIA computer security activities back on track:

° Reaffirm the basic responsibilities of the D/OS and the D/OIT as set forth in the joint OS/OIT memorandum of understanding of 31 December 1985.

° Create a joint OS/OIT task force to revise the implementation plan contained in the MOU. Set a tight timetable for creation of a more detailed and more realistic action plan. If appropriate, issue a revised MOU.

° Raise the organizational rank of computer security activities in OS from Division to Group level to increase visibility and priority. Insure strong leadership.

° Ask the D/OS to audit budget submissions to insure that component needs for computer security are adequately addressed. This should be done in full cooperation with components.

° Direct the D/OS to prepare a comprehensive, agency-wide information security plan in consonance with overall CIA planning for information processing. This plan should be prepared by a working group composed of representatives from all involved components.

25X1 [redacted]

~~SECRET~~

° Restore OS as a full member on the Information Systems Board.

° Strengthen CIA participation in community information security activities.

3. Background: As we sought to consolidate technical security activities in 1985, resolution of computer security responsibilities was one of our most difficult tasks. Earlier debate over the issue had resulted in the breakup of the former OS Information Systems Security Group (ISSG) into two components: the Information Security Group in OS and the Computer Security Group in OIT. For a multitude of reasons, the divided activity did not serve us well.

4. Dialogue between OS and OIT during the latter part of 1985 produced a joint Memorandum of Understanding (MOU), signed on 31 December 1985, that laid out a new working arrangement. (See attachment)

5. The key provisions of the 1985 MOU were:

a. A statement of common goals in protecting CIA information systems.

b. A recognition of the D/OS's responsibility to "develop and administer policy and doctrine" for information security.

c. A recognition of other central responsibilities of the D/OS in computer security.

d. A recognition of the D/OIT's responsibilities for the day-to-day security of CIA computer centers.

e. Specification of details of a plan to consolidate positions in OS to form a central computer security unit and to reallocate positions to form an expanded OIT computer security unit.

f. An assurance from OIT to allow OS access to OIT resources and to provide advice and consultation to OS.

g. An agreement to jointly review the threat to CIA information systems on an annual basis.

h. An agreement to work jointly to insure that adequate resources are allocated to computer security.

6. Just over a year has passed since the signing of the MOU and progress has been slow. We believe that the basic principles established in the MOU are still valid, but the implementation plan we laid out in the MOU (paragraph D) could have been better. We were probably too optimistic in our forecasts as to how quickly an expanded computer security unit could be established in OIT. Increased priority in OS and greater dialogue between the two offices might have produced faster results. Other details of the implementation plan may not have been practical. At the same time, leadership in OIT has changed and a move to place computer security under OIT's control is evident. Uncertainties at the working level are affecting progress. Dialogue between the offices is not what it should be.

7. We believe the secret to success in computer security will be to reaffirm the basic principles laid out in the MOU, reestablish a constructive dialogue between OS and OIT, and work out a practical new game plan for achieving our common goals.

8. The Basics: As with any other security discipline, computer security is a responsibility shared between OS and line components. The D/OS bears the central responsibility for formulating security policy, standards, and guidelines. He does this in consultation with line elements. He has established the Technical Security Policy Advisory Board, whose members are the Directors of offices involved in technical security, to assist him in formulating technical security policy.

9. It is the responsibility of line components to carry out policies established by the D/OS. They must institute appropriate procedures and monitor component activities on a daily basis to insure that security needs are met. They must plan for security in developmental activities and in operations and insure that adequate resources are available for security.

25X1 10. OS has assigned nearly [redacted] security officers at home and abroad to assist line components in carrying out security responsibilities. This force consists of security generalists, technical security personnel, and specialists such as polygraphers and protective officers. Representation is tailored to the needs of the component.

11. The D/OS must provide a check and balance on component security by continually assessing the state of security. He does this through the area officers and through special surveys and inspections. This is critical to insure that security is maintained at an appropriate level at all times, including those times when a component is faced with unusual operational demands and resource limitations.

12. The D/OS must also support line components by providing certain services of common concern, such as RDT&E, threat and vulnerability assessments, and training. He must help to insure that adequate resources are provided for security activities by planning, programming and budgeting for those resources not included in component programs.

13. We believe all of the above applies to computer security. We believe that, as provided in the MOU, the best solution to computer security is a strong, central unit in OS with strong, resident "area" computer security staffs to assist components in carrying out their computer security programs. OIT must have a robust staff to plan and monitor security activities and to insure that security is a component of developmental programs.

14. We continue to believe that we can provide the best personnel for computer security staffs through development and training in OS. We believe this to be true because computer security is one of the most complex security disciplines. It is not a "pure" security discipline. Some features are unique, involving very technical details of hardware and software. But many features involve linkages with other security disciplines: TEMPEST, technical surveillance countermeasures, physical security, information handling and control, COMSEC, and even personnel security. Careful personnel selection, training and development is key.

15. It is important that we move with resolve to correct our present difficulties with computer security. We must work toward a solution which will not only solve today's problems, but will provide a foundation for the future. I hope you will give serious consideration to our action plan.

25X1

[redacted]

Attachment

cc: D/OIT

ALL PORTIONS CLASSIFIED SECRET

ROUTING AND RECORD SHEET

SUBJECT: (Optional)

FROM: Director of Information Technology 2D00, Hqs.	EXTENSION [redacted]	NO.	DATE 8 January 1987

25X1

TO: (Officer designation, room number, and building)	DATE RECEIVED	DATE FORWARDED	OFFICER'S INITIALS	COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.)
1. DDA				Bill-- I didn't know whether to send you this officially or unofficially so I'll start with the unofficial route and wait for your guidance.
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				

D/OIT

ADMINISTRATIVE - INTERNAL USE ONLY

OIT 1063-86
0 5 JAN 1987

MEMORANDUM FOR: Deputy Director for Administration

FROM: Edward J. Maloney
Director of Information Technology

SUBJECT: Computer Security

1. I propose that responsibility for the entire computer security program of CIA be lodged with the Office of Information Technology (OIT). The current split between the Office of Security (OS) and OIT is not enhancing our computer security posture, and there is little prospect that the current structure will permit us to improve our situation.

2. We know from experience that when computer security personnel and responsibilities were more fully located in OIT, substantial interest in the issues grew throughout the office. There was regular, easy access for the computer security people in all OIT groups. The OIT program anticipated development activities that would include enhanced security as a major, embedded feature. There was good communication about technical requirements and the opportunities afforded by technology. The atmosphere was natural.

3. Since the return of the computer security function to OS, we have lost ground in many of these areas. [redacted] concerns in OS clearly overshadow computer security interests. "We-they" has set in between OS and OIT, even with substantial coaching to avoid it. Communication is poorer because each "side" feels it has a specific mandate to carry out its mission as it sees fit. Integration of interests and efforts is lost for all intents and purposes. Little has been done outside OIT to enhance computer security at the technology level, though customer education has improved as an area of joint rather than divided activity.

STAT

4. I propose to create a Computer Security Activity in OIT that reports directly to the Office Director. It would be the only such reporting relationship in the office. I will install a leader at the SIS level who will coordinate office-wide computer security efforts in development, technology procurement, research, auditing, policy, and education. I envision the activity including all elements of OS/ISSG, those activities in OIT now devoted in whole or in substantial part to this function, and new positions to be added in FY88 and 89. I believe that this is the only way for us to move ahead smartly, especially at a time of resource constraint.

ADMINISTRATIVE - INTERNAL USE ONLY

SUBJECT: Computer Security

5. The personnel and resources from this merger and growth would be allocated within OIT mainly at the group level, rather than holding them as a large central structure. The computer security industrial audit teams would work with our Domestic Field Group's COMSEC audit teams to perform joint technical audits, and more frequent audits than either group can do now. We are at substantial risk on industrial audits as things now stand. The Audit and Education Branch of OIT would remain intact, but also responsive to the Activitiy Chief/Coordinator. A function like the PC encryption board project (a subset of PC computer security) might well reside in NSEG, etc.

6. This proposal promises both measurable progress in this area and better management. The resources programmed for computer security by OS, those that I am prepared to commit, and a substantially more integrated management of all computer security resources, should give us the basis for a serious attack on this problem.

[redacted]

Edward J. Maloney

ORIG: DD/OIT-M/[redacted] Jan 87

Distribution:

Original - Addressee
1 - OIT Chrono
1 - Technical Sec. File
2 - OIT Registry